JOURNAL OF ALGEBRA 16, 271–297 (1970)

Affine Hopf Algebras II

ROBERT G. HEYNEMAN AND MOSS E. SWEEDLER*

University of North Carolina, Cornell University

Communicated by D. Buchsbaum

Received June 9, 1969

It is well known that if G is an affine algebraic group defined over a field k of characteristic zero, then the identity of G is a non-singular point. The usual proof is that G has some non-singular point g. Translating by g^{-1} shows that the identity must be non-singular. We show that if the characteristic is zero and G is an affine algebraic monoid—group without inverses, such as $M(n, k)$ the $n \times n$-matrix monoid under multiplication—then the identity of G is non-singular. When G does have inverses we easily deduce that A the coordinate ring of G is reduced.

In Affine Hopf Algebras I we introduced $\mathscr{D}$ the ring of invariant differential operators on A. $\mathscr{D}$ is a cocommutative connected Hopf algebra which is sometimes called the "hyperalgebra" of the algebraic monoid. The algebra $\mathscr{D}^*$ which is the linear dual to $\mathscr{D}$ is algebra isomorphic to $\hat{A}$ the completion of the local ring at the identity of G. Thus the coalgebra structure of $\mathscr{D}$ is of basic interest.

We show that when the characteristic is zero $\mathscr{D}$ is coalgebra isomorphic to $B(U)$ a certain coalgebra of "divided powers." $B(U)$ has a well determined coalgebra structure. (Actually $\mathscr{D}$ is the universal enveloping algebra of $P(\mathscr{D})$ its Lie algebra of primitive elements which is the Lie algebra of G. We do not reprove this result of Kostant which has appeared elsewhere.)

Primarily this paper is concerned with studying the coalgebra structure of $\mathscr{D}$ when the characteristic is $p > 0$. Results for characteristic zero have been included when they easily "fell out" of the general theory. The first section of the paper develops the $\mathscr{V}$ map for cocommutative coalgebras. This is a $1/p$-linear map which is dual to the Frobenius (p-power) map. If C is a cocommutative coalgebra then $\mathscr{V}$ is a map from C to $C \otimes_k k^{1/p}$. $\mathscr{V}$ commutes with coalgebra maps and has all the properties one would expect from its being dual to the Frobenius map.

In Section 2 we study a general cocommutative connected bialgebra $\mathscr{D}$. For any such $\mathscr{D}$ there is a vector space U and an injective coalgebra map

* The second author supported in part by NSF GP 7945.

$\varphi : \mathscr{D} \to B(U)$. We get at the coalgebra structure of $\mathscr{D}$ through the coalgebra structure of $\operatorname{Im} \varphi$. This is made easier by the convenient basis of $B(U)$. The main result is that $\mathscr{D} \simeq B(U)$ as coalgebras if and only if $\mathscr{V} : \mathscr{D} \to \mathscr{D} \otimes_k k^{1/p}$ is surjective. Other equivalent conditions are that $\operatorname{Hom}_{k^{1/p}}(\mathscr{D} \otimes_k k^{1/p}, k^{1/p})$ is a domain; $\operatorname{Hom}_{k^{1/p}}(\mathscr{D} \otimes_k k^{1/p}, k^{1/p})$ is reduced; each primitive element of $\mathscr{D}$ lies in an infinite sequence of divided powers. If U has finite dimension n then $B(U)^*$ is a power-series ring in n variables over k.

In the third section we let $\mathscr{D}$ be the hyperalgebra of an affine algebraic monoid. We show that $\mathscr{D}$ "commutes" with field extension and that $\hat{A}$ is a power-series ring if and only if $\mathscr{D} \simeq B(U)$ as coalgebras. We prove the initial remarks about affine algebraic monoids in characteristic zero. When the characteristic is greater than zero we give four conditions equivalent to $\hat{A}$ being a power-series ring over k. We show that these conditions are satisfied when A is "absolutely" reduced. Conversely we show that if G is a group then $\hat{A}$ being a power-series ring over k implies that A is absolutely reduced.

This paper is a continuation of Affine Hopf Algebras I. That is why it begins with Chapter 4. A citation "$(x \cdot y \cdot z)$" can be found in Affine Hopf Algebras I whenever $x \leqslant 3$.

4.1 *The $\mathscr{V}$ Map*

Let X be a vector space over k and $\mathfrak{S}_n$ the symmetric group on n-letters. Consider $\otimes^n X$ as an $\mathfrak{S}_n$-module by setting

$$\sigma(x_1 \otimes \cdots \otimes x_n) = x_{1\sigma} \otimes \cdots \otimes x_{n\sigma},$$

for $\sigma \in \mathfrak{S}_n$. $\mathscr{S}^n X$ the symmetric tensors in $\otimes^n X$ equals

$$\left\{ y \in \bigotimes^n X \;\middle|\; \sigma \cdot y = y \text{ for all } \sigma \in \mathfrak{S}_n \right\}.$$

We let $S^n X$ denote the nth symmetric power of X. This is precisely the nth graded component of the symmetric algebra. We use ι and π to denote the natural inclusion and projection

$$\mathscr{S}^n X \xrightarrow{\iota} \bigotimes^n X$$

$$\bigotimes^n X \xrightarrow{\pi} S^n X.$$

If L is a field extension of k we can form $X \otimes_k L$ the scalar extension of X to L. The symmetric algebra $S_L(X \otimes_k L)$ *over* L of $X \otimes_k L$ is naturally isomorphic to $(SX) \otimes_k L$ as a graded L-algebra. SX is the symmetric algebra of X over k. We freely identify $(SX) \otimes_k L$ and $S_L(X \otimes_k L)$ and we identify the nth graded component $(S^n X) \otimes_k L$ with $S_L{}^n(X \otimes_k L)$.

Let $\bar{k}$ denote an algebraic closure of k and let $k^{1/p}$ denote $\{\lambda \in \bar{k} \mid \lambda^p \in k\}$. When the characteristic of k is $p > 0$ then $k^{1/p}$ is the maximal exponent one purely inseparable extension of k. If A is an algebra over $k^{1/p}$ we may consider A as an algebra over k since $k \subset k^{1/p}$. Let $A^{(p)}$ denote $\{a^p \in A \mid a \in A\}$. If A is commutative then $A^{(p)}$ is a k subalgebra of A. If A happens to be $(SX) \otimes_k k^{1/p}$ it has the k subalgebra SX and $[(SX) \otimes_k k^{1/p}]^{(p)} \subset SX$ as a subalgebra.

Let $F : X \otimes_k k^{1/p} \to S^p X$ be defined by $y \mapsto y^p$. Then F is an injective p-linear map.

4.1.1. THEOREM. *Suppose the characteristic of k is $p > 0$ and X is a vector space over k.*

(a) *There is a $1/p$-linear map $V : \mathscr{S}^p X \to X \otimes_k k^{1/p}$ making the following diagram commute*

$$\begin{array}{ccc} \mathscr{S}^p X & \xrightarrow{\iota} & \overset{p}{\bigotimes} X \\ {\scriptstyle V}\big\downarrow & & \big\downarrow{\scriptstyle \pi} \\ X \otimes k^{1/p} & \xrightarrow{F} & S^p X. \end{array}$$

(b) *For any $y \in \mathscr{S}^p X$, the element $V(y) \in X \otimes_k k^{1/p}$ is the unique element in $X \otimes_k k^{1/p}$ with $\pi\iota(y) = F(V(y))$.*

Proof. (b) Suppose V exists making the diagram commute. The injectivity of F guarantees $V(y)$ is the unique element of $X \otimes_k k^{1/p}$ with $\pi\iota(y) = F[V(y)]$ for any $y \in \mathscr{S}^p X$.

(a) Let B be a basis for X and let $P = \{1,..., p\}$. For $f \in B^P$ i.e. $f : P \to B$, let $(f) = f(1) \otimes \cdots \otimes f(p) \in \otimes^p X$. Totally order B and call $f \in B^P$ *ordered* if $f(1) \leqslant f(2) \leqslant \cdots \leqslant f(p)$. By Orb$(f)$ we denote

$$\left\{ y \in \overset{p}{\bigotimes} X \,\middle|\, y = \sigma \cdot (f) \text{ for some } \sigma \in \mathfrak{S}_p \right\}.$$

By Sym(f) we denote

$$\Sigma y (y \in \mathrm{Orb}(f)).$$

The following results are standard or easy to prove:

1. $\{(f) \mid f \in B^P\}$ is a basis for $\otimes^p X$.

2. For $f \in B^P$ the cardinality of Orb(f) is divisible by p if f is not constant and the cardinality of Orb(f) is one if f is constant, i.e., $f(1) = f(2) = \cdots = f(p)$.

3. For any $f \in B^p$ there is a unique ordered $g \in B^p$ with $(g) \in \mathrm{Orb}(f)$.
4. $\{\mathrm{Sym}(f) \mid f \in B^p \text{ and } f \text{ is ordered}\}$ is a basis for $\mathscr{S}^p X$.

Define $V : \mathscr{S}^p X \to X \otimes_k k^{1/p}$ to be the $1/p$-linear map determined by $V(\mathrm{Sym}(f)) = 0$ if f is ordered and f is not constant; $V(\mathrm{Sym}(f)) = f(1) \otimes 1$ if f is ordered and f is constant. Since V is $1/p$-linear and F is p-linear it follows that FV is linear. Thus to prove that the diagram commutes it suffices to check on a basis for $\mathscr{S}^p X$.

For $f \in B^p$ a constant function $\mathrm{Sym}(f) = f(1) \otimes \cdots \otimes f(p) = f(1) \otimes \cdots \otimes f(1)$ and $\pi\iota(\mathrm{Sym}(f)) = f(1)^p = F(f(1) \otimes 1) = F(V(\mathrm{Sym}(f))$. For $f \in B^p$ ordered but not constant let $\mathrm{Orb}(f) = (g_1),\dots,(g_{pr})$ with $\{g_i\} \subset B^p$. Clearly $\pi(g_1) = \cdots = \pi(g_{pr})$ so that $\pi\iota(\mathrm{Sym}(f)) = pr\pi(g_1) = 0 = F(0) = FV(\mathrm{Sym}(f))$. This concludes the proof.

4.1.2. COROLLARY TO THE PROOF. *V is given explicitly by*

$$V(\mathrm{Sym}(f)) = \begin{cases} 0 & \text{if } f \text{ is not constant} \\ f(1) \otimes 1 & \text{if } f \text{ is constant,} \end{cases}$$

for ordered $f \in B^p$.

Suppose both X and Y are vector spaces over k and $G : X \to Y$ is a linear map. G induces $G \otimes I : X \otimes_k k^{1/p} \to Y \otimes_k k^{1/p}$ and $\otimes^n G : \otimes^n X \to \otimes^n Y$. We define $\mathscr{S}^n G$ as the unique linear map making commute

$$\begin{array}{ccc} \mathscr{S}^n X & \xrightarrow{\mathscr{S}^n G} & \mathscr{S}^n Y \\ \downarrow{\scriptstyle \iota} & & \downarrow{\scriptstyle \iota} \\ \overset{n}{\bigotimes} X & \xrightarrow{\otimes^n G} & \overset{n}{\bigotimes} Y. \end{array}$$

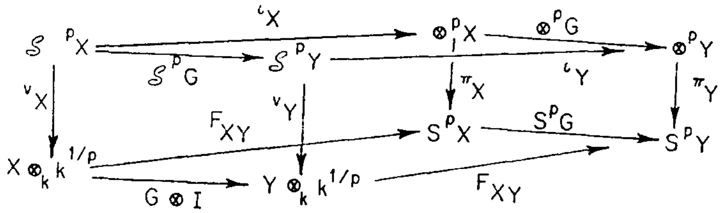
$\mathscr{S}^n G$ exists because $\otimes^n G(\mathscr{S}^n X) \subset \mathscr{S}^n Y$.

4.1.3. Suppose the characteristic of k is $p > 0$ and $G : X \to Y$ is a linear map, then the following diagram commutes:

$$\begin{array}{ccc} \mathscr{S}^p X & \xrightarrow{\mathscr{S}^p G} & \mathscr{S}^p Y \\ \downarrow{\scriptstyle V_X} & & \downarrow{\scriptstyle V_Y} \\ X \otimes_k k^{1/p} & \xrightarrow{G \otimes I} & Y \otimes_k k^{1/p}. \end{array}$$

Proof. $G : X \to Y$ induces a graded algebra map $SG : SX \to SY$. We denote by $S^n G$ the restriction $SG \mid S^n X : S^n X \to S^n Y$. Then $S^1 G = G$.

It is clear that in the following block diagram all faces other than the front square commute:



This implies that

$$F_Y(G \otimes I)\, V_X = F_Y V_Y(\mathscr{S}^p G).$$

Since F_Y is injective we have that $(G \otimes I)\, V_X = V_Y(\mathscr{S}^p G)$ which proves the proposition.

Suppose X and Y are vector spaces over k. We have the linear isomorphism

$$\alpha^n\colon \Big(\bigotimes^n X\Big) \otimes \Big(\bigotimes^n Y\Big) \xrightarrow{\cong} \bigotimes^n (X \otimes Y)$$
$$x_1 \otimes \cdots \otimes x_n \otimes y_1 \otimes \cdots \otimes y_n \to x_1 \otimes y_1 \otimes \cdots \otimes x_n \otimes y_n .$$

We define β^n as the unique linear map making commute

$$\begin{array}{ccc} (\mathscr{S}^n X) \otimes (\mathscr{S}^n Y) & \xrightarrow{\beta^n} & \mathscr{S}^n(X \otimes Y) \\ \big\downarrow{\scriptstyle \iota\otimes\iota} & & \big\downarrow{\scriptstyle \iota} \\ \Big(\bigotimes^n X\Big) \otimes \Big(\bigotimes^n Y\Big) & \xrightarrow{\alpha^n} & \bigotimes^n (X \otimes Y). \end{array}$$

β^n exists because $\alpha^n[(\mathscr{S}^n X) \otimes (\mathscr{S}^n Y)] \subset \mathscr{S}^n(X \otimes Y)$.

4.1.4. Proposition. *Suppose the characteristic of k is $p > 0$ and X and Y are vector spaces over k. Then*

$$\begin{array}{ccc} (\mathscr{S}^p X) \otimes_k (\mathscr{S}^p Y) & \xrightarrow{\beta^p} & \mathscr{S}^p(X \otimes_k Y) \\ \big\downarrow{\scriptstyle V_X \otimes V_Y} & & \big\downarrow{\scriptstyle V_{X\otimes Y}} \\ (X \otimes k^{1/p}) \otimes_{k^{1/p}} (Y \otimes k^{1/p}) & \xrightarrow{\cong} & X \otimes_k Y \otimes_k k^{1/p} \end{array}$$

is a commutative diagram. (We explain below why $V_X \otimes V_Y$ is well defined.)

Proof. The map

$$(\mathscr{S}^p X) \times (\mathscr{S}^p Y) \to (X \otimes_k k^{1/p}) \otimes_{k^{1/p}} (Y \otimes_k k^{1/p})$$
$$v \times w \mapsto V_X(v) \otimes V_{.}\,(w)$$

is biadditive and balanced [1, p. 74]. Thus there exists a unique ($1/p$-linear) map $V_X \otimes V_Y : (\mathcal{S}^p X) \otimes_k (\mathcal{S}^p Y) \to (X \otimes_k k^{1/p}) \otimes_{k^{1/p}} (Y \otimes_k k^{1/p})$ given by $\sum v_i \otimes w_i \to \sum V_X(v_i) \otimes V_Y(w_i)$. Similarly there is a unique p-linear map $F_X \otimes F_Y : (X \otimes_k k^{1/p}) \otimes_{k^{1/p}} (Y \otimes_k k^{1/p}) \to S^p X \otimes_k S^p Y$ given by $\sum u_i \otimes z_i \to \sum F_X(u_i) \otimes F_Y(z_i)$. Although F_X is not linear it is p-linear and one can easily verify that F_X being injective is equivalent to F_X carrying $k^{1/p}$-linearly independent sets in $X \otimes_k k^{1/p}$ to k-linearly independent sets in $S^p X$. Similarly for F_Y. Thus $F_X \otimes F_Y$ carries $k^{1/p}$-linearly independent sets in $(X \otimes_k k^{1/p}) \otimes_{k^{1/p}} (Y \otimes_k k^{1/p})$ to k-linearly independent sets in $S^p X \otimes_k S^p Y$ and $F_X \otimes F_Y$ is injective.

The composite

$$\bigotimes_k^p (X \otimes_k Y) \xrightarrow{(\alpha^p)^{-1}} \Big(\bigotimes_k^p X\Big) \otimes_k \Big(\bigotimes_k^p Y\Big) \xrightarrow{\pi_X \otimes \pi_Y} (S^p X) \otimes_k (S^p Y)$$

is a symmetric function on $\otimes_k^p (X \otimes_k Y)$, so factors through $S^p(X \otimes_k Y)$. This gives the map

$$\gamma^p : S^p(X \otimes_k Y) \to (S^p X) \otimes_k (S^p Y)$$
$$(x_1 \otimes y_1)(x_2 \otimes y_2) \cdots (x_p \otimes y_p) \to (x_1 x_2 \cdots x_p) \otimes (y_1 y_2 \cdots y_p)$$

which makes commute:

$$\begin{tikzcd}
\Big(\bigotimes_k^p X\Big) \otimes_k \Big(\bigotimes_k^p Y\Big) \arrow[r, "\alpha^p"] \arrow[d, "\pi_X \otimes \pi_Y"] & \bigotimes_k^p (X \otimes_k Y) \arrow[d, "\pi_{X \otimes Y}"] \\
(S^p X) \otimes_k (S^p Y) & S^p(X \otimes_k Y). \arrow[l, "\gamma^p"']
\end{tikzcd}$$

Thus in the block diagram all faces other than the front square commute:

$$\begin{tikzcd}
& (\otimes_k^p X) \otimes_k (\otimes_k^p Y) \arrow[rr, "\alpha^p"] \arrow[d, "\pi_X \otimes \pi_Y"] & & \otimes_k^p (X \otimes_k Y) \arrow[d, "\pi_{X \otimes Y}"] \\
& (S^p X) \otimes_k (S^p Y) & & S^p (X \otimes_k Y) \arrow[ll, "\gamma^p"'] \\
(\mathcal{S}^p X) \otimes_k (\mathcal{S}^p Y) \arrow[uur, "\iota_X \otimes \iota_Y"] \arrow[rr, "\beta^p"] \arrow[d, "V_X \otimes V_Y"'] & & \mathcal{S}^p (X \otimes_k Y) \arrow[uur, "\iota_{X \otimes Y}"] \arrow[d, "V_{X \otimes Y}"] & \\
(X \otimes_k k^{1/p}) \otimes_{k^{1/p}} Y \otimes_k k^{1/p}) \arrow[uur, "F_X \otimes F_Y"] & & X \otimes_k Y \otimes_k k^{1/p} \arrow[ll, "\cong"'] \arrow[uur, "F_{X \otimes Y}"'] &
\end{tikzcd}$$

This implies that

$$(F_X \otimes F_Y)(V_X \otimes V_Y) = (F_X \otimes F_Y)(\cong)(V_{X \otimes Y})\beta^p.$$

Since $F_X \otimes F_Y$ is injective we have that the front square commutes. Then the front square commutes with the isomorphism at the bottom replaced by its inverse isomorphism and we are done.

Let C be a cocommutative coalgebra and $\Delta_{n-1} : C \to \otimes^n C$ be iterated diagonalization. Since C is cocommutative $\operatorname{Im} \Delta_{n-1} \subset \mathscr{S}^n C$. We let $\bar{\Delta}_{n-1}$ denote Δ_{n-1} with its image restricted to $\mathscr{S}^n C$.

DEFINITION. If the characteristic of k is $p > 0$ and C is a cocommutative coalgebra over k we define $\mathscr{V} : C \to C \otimes_k k^{1/p}$ as the $1/p$-linear map which is the composite:

$$C \xrightarrow{\bar{\Delta}_{p-1}} \mathscr{S}^p C \xrightarrow{V} C \otimes k^{1/p}.$$

4.1.5. PROPOSITION. *Let C and D be cocommutative coalgebras over k, $G : C \to D$ a coalgebra map and assume the characteristic of k is $p > 0$.*

(a) *The following diagram commutes:*

$$\begin{array}{ccc} C & \xrightarrow{G} & D \\ \downarrow{\scriptstyle \mathscr{V}_C} & & \downarrow{\scriptstyle \mathscr{V}_D} \\ C \otimes_k k^{1/p} & \xrightarrow{G \otimes I} & D \otimes_k k^{1/p}. \end{array}$$

(b) *If $C \otimes_k D$ has the tensor product coalgebra structure then the diagram*

$$\begin{tikzcd} & C \otimes D \arrow[dl, "\mathscr{V}_{C \otimes D}"'] \arrow[dr, "\mathscr{V}_C \otimes \mathscr{V}_D"] & \\ (C \otimes_k D) \otimes_k k^{1/p} & & (C \otimes_k k^{1/p}) \otimes_{k^{1/p}} (D \otimes_k k^{1/p}) \arrow[ll, "\cong"'] \end{tikzcd}$$

commutes. (We explain below why $\mathscr{V}_C \otimes \mathscr{V}_D$ is well defined.)

(c) *If $C \oplus D$ has the direct sum coalgebra structure then the diagram*

$$\begin{tikzcd} & C \oplus D \arrow[dl, "\mathscr{V}_{C \oplus D}"'] \arrow[dr, "\mathscr{V}_C \oplus \mathscr{V}_D"] & \\ (C \oplus D) \otimes_k k^{1/p} \arrow[rr, "\cong"] & & (C \otimes_k k^{1/p}) + (D \otimes_k k^{1/p}) \end{tikzcd}$$

commutes.

Proof. (a) Since G is a coalgebra map we have that $\Delta_{D(p-1)}G = (\otimes^p G)\,\Delta_{C(p-1)}$. Thus $\bar{\Delta}_{D(p-1)}G = (\mathscr{S}^p G)\,\bar{\Delta}_{C(p-1)}$ and

$$\begin{aligned}\mathscr{V}_D G &= V_D\bar{\Delta}_{D(p-1)}G = V_D(\mathscr{S}^p G)\,\bar{\Delta}_{C(p-1)}\\ &= (G\otimes I)\,V_C\bar{\Delta}_{C(p-1)} \qquad \text{(by 4.1.3)}\\ &= (G\otimes I)\,\mathscr{V}_C.\end{aligned}$$

(b) The map $C \times D \to (C \otimes_k k^{1/p}) \otimes_{k^{1/p}} (D \otimes_k k^{1/p})$ given by $c \times d \mapsto \mathscr{V}_C(c) \otimes \mathscr{V}_D(d)$ is biadditive and balanced, [1, p. 74]. Thus there exists a unique ($1/p$-linear) map $\mathscr{V}_C \otimes \mathscr{V}_D : C \otimes D \to (C \otimes_k k^{1/p}) \otimes_{k^{1/p}} (D \otimes_k k^{1/p})$ where $\sum c_i \otimes d_i \mapsto \sum \mathscr{V}_C(c_i) \otimes \mathscr{V}_D(d_i)$. In the diagram below the top triangle commutes because $C \otimes D$ has the tensor product coalgebra structure and the trapezoid commutes by 4.1.4.

$$\begin{tikzcd}
 & C\otimes_k D \arrow[dl, "\bar{\Delta}_{(C\otimes D)(p-1)}"'] \arrow[dr, "\bar{\Delta}_{C(p-1)}\otimes\bar{\Delta}_{D(p-1)}"] & \\
\mathscr{S}^p(C\otimes_k D) \arrow[d, "V_{C\otimes D}"'] & & (\mathscr{S}^pC)\otimes_k(\mathscr{S}^pD) \arrow[ll, "\beta^p"'] \arrow[d, "V_C\otimes V_D"] \\
C\otimes_k D\otimes_k k^{1/p} & & (C\otimes_k k^{1/p})\otimes_{k^{1/p}}(D\otimes_k k^{1/p}). \arrow[ll, "\cong"']
\end{tikzcd}$$

Thus the outer triangle commutes. The left leg is $\mathscr{V}_{C\otimes D}$ and the right leg is $\mathscr{V}_C \otimes \mathscr{V}_D$ proving (b).

(c) Since $C \xrightarrow{\lambda} C \oplus D$, $c \mapsto (c, 0)$ is a coalgebra map, (a) implies that

$$\begin{tikzcd}
C \arrow[r, "\lambda"] \arrow[d, "\mathscr{V}_C"'] & C\oplus D \arrow[d, "\mathscr{V}_{C\oplus D}"] \\
C\otimes_k k^{1/p} \arrow[r, "\lambda\otimes I"] & (C\oplus D)\otimes_k k^{1/p}
\end{tikzcd}$$

is commutative. Identifying $(C \oplus D) \otimes_k k^{1/p}$ with $(C \otimes_k k^{1/p}) \oplus (D \otimes_k k^{1/p})$ makes $\lambda \otimes I$ correspond to $\bar{c} \mapsto (\bar{c}, 0)$. Similarly for D and $\mathscr{V}_D$. This with the additivity of $\mathscr{V}_{C\oplus D}$ gives (c). Q.E.D.

The next proposition shows that $\mathscr{V}$ respects the coalgebra structure as well as possible additional structure.

4.1.6. Proposition. *Suppose the characteristic of k is $p > 0$ and C is a cocommutative coalgebra.*

(a) *If $C \otimes_k k^{1/p}$ is considered as a $k^{1/p}$ coalgebra via scalar extension then*

$$\begin{tikzcd} C \arrow[r, "\Delta_C"] \arrow[d, "\mathscr{V}_C"'] & C \otimes C \arrow[d, "\mathscr{V}_C \otimes \mathscr{V}_C"] \\ C \otimes_k k^{1/p} \arrow[r, "\Delta_{C \otimes_k k^{1/p}}"'] & (C \otimes_k k^{1/p}) \otimes_{k^{1/p}} (C \otimes_k k^{1/p}) \end{tikzcd}$$

commutes.

(b) *$\mathscr{V}_k : k \to k^{1/p}$ is the map $\tau \to \tau^{1/p}$ for all $\tau \in k$.*

(c) *The diagram*

$$\begin{tikzcd} C \arrow[r, "\epsilon"] \arrow[d, "\mathscr{V}_C"'] & k \arrow[d, "\mathscr{V}_k"] \\ C \otimes_k k^{1/p} \arrow[r, "\epsilon_{C \otimes k^{1/p}}"'] & k^{1/p} \end{tikzcd}$$

commutes.

(d) *If C is a bialgebra and $C \otimes_k k^{1/p}$ has the scalar extension $k^{1/p}$-bialgebra structure then the diagram*

$$\begin{tikzcd} C \otimes C \arrow[r, "p_C"] \arrow[d, "\mathscr{V}_C \otimes \mathscr{V}_C"'] & C \arrow[d, "\mathscr{V}_C"] \\ (C \otimes_k k^{1/p}) \otimes_{k^{1/p}} (C \otimes_k k^{1/p}) \arrow[r, "p_{C \otimes_k k^{1/p}}"'] & C \otimes_k k^{1/p} \end{tikzcd}$$

and

$$\begin{tikzcd} k \arrow[r, "\eta"] \arrow[d, "\mathscr{V}_k"'] & C \arrow[d, "\mathscr{V}_C"] \\ k^{1/p} \arrow[r, "\eta_{C \otimes_k k^{1/p}}"] & C \otimes_k k^{1/p} \end{tikzcd}$$

commute.

(e) *If C is a Hopf algebra and $C \otimes k^{1/p}$ has the scalar extension Hopf algebra structure then the diagram*

$$\begin{tikzcd} C \arrow[r, "S"] \arrow[d, "\mathscr{V}_C"'] & C \arrow[d, "\mathscr{V}_C"] \\ C \otimes_k k^{1/p} \arrow[r, "S_{C \otimes_k k^{1/p}}"'] & C \otimes_k k^{1/p} \end{tikzcd}$$

commutes.

Proof. (a), (c), (d) and (e) follow from (4.1.5, a, b) and the fact that $\epsilon, \Delta, p, \eta, S$ are coalgebra morphisms. (Δ, S are coalgebra morphisms because C is cocommutative.)

(b) The spaces $\mathscr{S}^p k$, $\otimes^p k$ and $S^p k$ are all naturally isomorphic to k and the maps $\mathscr{S}^p k \xrightarrow{\iota} \otimes^p k$, $\otimes^p k \xrightarrow{\pi} S^p k$ correspond to the identity map. The map $k^{1/p} = k \otimes_k k^{1/p} \xrightarrow{F} S^p k = k$ is just the pth power map. Thus $k = \mathscr{S}^p k \xrightarrow{V} k \otimes_k k^{1/p} = k^{1/p}$ must be the pth-root map if

$$\begin{array}{ccc} k & \xrightarrow{I\sim\iota} & k \\ {\scriptstyle V}\big\downarrow & & \big\downarrow{\scriptstyle I\sim\pi} \\ k^{1/p} & \xrightarrow[p\text{-power}\sim F]{} & k \end{array}$$

is to commute. $\bar{\Delta}_{p-1} : k \to \mathscr{S}^p k = k$ is just the identity map and so the composite $\mathscr{V}_k$

$$k \xrightarrow{I\sim\bar{\Delta}_{p-1}} k \xrightarrow{p\text{-root}\sim V} k^{1/p}$$

is the p-root map. Q.E.D.

Suppose A is a commutative algebra over $k^{1/p}$. Let $\mathscr{F} : A \to A^{(p)}$ be the map $a \mapsto a^p$. Consider $C \subset C \otimes_k k^{1/p}$ via the inclusion $c \to c \otimes 1$.

4.1.7. THEOREM. *Let A be a commutative $k^{1/p}$-algebra and*

$$f \in \operatorname{Hom}_{k^{1/p}}(C \otimes_k k^{1/p}, A)$$

where C is a cocommutative coalgebra over k.

(a) *$f^p(c) = \mathscr{F}\{f[\mathscr{V}(c)]\}$ for all $c \in C$. Here f^p denotes the product of f with itself p-times in the $k^{1/p}$-algebra* $\operatorname{Hom}_{k^{1/p}}(C \otimes_k k^{1/p}, A)$.

(b) *Suppose $A = k^{1/p}$ and B is a subset of* $\operatorname{Hom}_{k^{1/p}}(C \otimes_k k^{1/p}, k^{1/p})$ *which is dense in the sense that if $0 \neq x \in C \otimes_k k^{1/p}$ then there is $f \in B$ with $f(x) \neq 0$. For any $c \in C$, $\mathscr{V}(c)$ is the unique element in $C \otimes_k k^{1/p}$ such that $f^p(c) = \mathscr{F}\{f[\mathscr{V}(c)]\}$ for all $f \in B$.*

Proof. To begin we consider C as a vector space and take SC the symmetric algebra on C over k. Form $(SC) \otimes_k k^{1/p}$ the scalar extension of SC to $k^{1/p}$ which we identify with $S_{k^{1/p}}(C \otimes_k k^{1/p})$ the symmetric algebra on $C \otimes_k k^{1/p}$ over $k^{1/p}$. Let $\rho \in \operatorname{Hom}_{k^{1/p}}(C \otimes_k k^{1/p}, (SC) \otimes_k k^{1/p})$ be the natural identification of $C \otimes_k k^{1/p}$ with the first graded component $(S^1 C \otimes_k k^{1/p})$ of $(SC) \otimes_k k^{1/p}$. We shall show that for any $c \in C$, $\mathscr{V}(c)$ is the unique element in $C \otimes_k k^{1/p}$ where $\rho^p(c) = \mathscr{F}(\rho(\mathscr{V}(c)))$.

One can easily check that $\rho^p(c)$ is the image of c under the composite $C \xrightarrow{\bar{\Delta}_{p-1}} \mathscr{S}^p C \xrightarrow{\pi\iota} S^p C \subset S^p C \otimes_k k^{1/p}$. By (4.1.1) $\mathscr{V}(c) = V\bar{\Delta}_{p-1}(c)$ is the unique element of $C \otimes_k k^{1/p}$ with $\mathscr{F}\{\rho[\mathscr{V}(c)]\} = FV(\bar{\Delta}_{p-1}(c)) = \pi\iota(\bar{\Delta}_{p-1}(c)) = \rho^p(c)$.

(a) Given $f \in \mathrm{Hom}_{k^{1/p}}(C \otimes_k k^{1/p}, A)$ it induces a unique algebra map $\bar{f} : (SC \otimes_k k^{1/p}) \to A$ where $\bar{f} \mid (C \otimes_k k^{1/p}) = f$. By the remarks at the beginning of Section 1.5, we see that

$$\mathrm{Hom}_{k^{1/p}}(C \otimes k^{1/p}, (SC) \otimes_k k^{1/p}) \xrightarrow{\varphi} \mathrm{Hom}_{k^{1/p}}(C \otimes_k k^{1/p}, A)$$
$$g \longrightarrow \bar{f}g$$

is an algebra map. Clearly $\varphi(\rho) = f$ and since φ is an algebra map

$$\varphi(\rho^p) = \varphi(\rho)^p = f^p; \qquad \text{i.e.,} \quad \bar{f}\rho^p = f^p.$$

Thus for each $c \in C$

$$f^p(c) = \bar{f}\rho^p(c) = \bar{f}\mathscr{F}(\rho(\mathscr{V}(c))).$$

Since $\mathscr{F}$ is the pth power map it commutes with the algebra homomorphism $\bar{f}$ and the right hand side is equal to

$$\mathscr{F}(\bar{f}\rho(\mathscr{V}(c))) = \mathscr{F}(f(\mathscr{V}(c))).$$

This proves (a).

(b) We know by (a) that for $c \in C$ and any $f \in \mathrm{Hom}_{k^{1/p}}(C \otimes_k k^{1/p}, k^{1/p})$

$$f^p(c) = \mathscr{F}(f(\mathscr{V}(c))).$$

Suppose $x \in C \otimes_k k^{1/p}$ and for all $f \in B$

$$f^p(c) = \mathscr{F}(f(x)).$$

Then

$$\mathscr{F}(f(\mathscr{V}(c))) = \mathscr{F}(f(x))$$

for all $f \in B$. If $\mathscr{V}(c) \neq x$ there is $f \in B$ with $f(\mathscr{V}(c)) \neq f(x)$ by the density of B. Since raising to the pth-power is injective in a field, $\mathscr{F}(f(\mathscr{V}(c)) \neq \mathscr{F}(f(x))$. Thus x must be equal to $\mathscr{V}(c)$.

4.1.8. Corollary. *If $A \neq \{0\}$ then for any $c \in C$, $\mathscr{V}(c)$ is the unique element in $C \otimes_k k^{1/p}$ such that*

$$f^p(c) = \mathscr{F}(f(\mathscr{V}(c))) \qquad \text{for all} \quad f \in \mathrm{Hom}_{k^{1/p}}(C \otimes_k k^{1/p}, A).$$

Proof. Since $A \neq \{0\}$, $k^{1/p} \xrightarrow{\eta} A$ is injective and induces an algebra injection $\mathrm{Hom}_{k^{1/p}}(C \otimes_k k^{1/p}, k^{1/p}) \hookrightarrow \mathrm{Hom}(C \otimes_k k^{1/p}, A)$ which we take for an identification. By (b) of the theorem the corollary is true even if we limit the maps to lie in the subalgebra $\mathrm{Hom}_{k^{1/p}}(C \otimes_k k^{1/p}, k^{1/p})$ of $\mathrm{Hom}_{k^{1/p}}(C \otimes_k k^{1/p}, A)$. Q.E.D.

We recall that a (possibly infinite) sequence of elements $\{c_0, c_1, ...\}$ in a coalgebra C is called a sequence of *divided powers* if $c_0 \neq 0$ and for each c_n in the sequence

$$\Delta(c_n) = \sum_{i=0}^{n} c_i \otimes c_{n-i}.$$

If the sequence is finite and consists of $\{c_0, ..., c_n\}$ it is called an n-sequence of divided powers. If the sequence is infinite it is called an ∞-sequence of divided powers.

4.1.9. PROPOSITION. *Suppose C is a cocommutative coalgebra, the characteristic of k is $p > 0$ and $\{c_i\}$ is an M-sequence of divided powers contained in C, $0 \leqslant M \in \mathbb{Z}$ or $M = \infty$. Then for each c_n in the sequence*

$$\mathscr{V}_C(c_n) = \begin{cases} 0 & \text{if } p \nmid n \\ c_{n/p} \otimes 1 & \text{if } p \mid n \end{cases}$$

Proof. Given an integer n let V be a vector space over k with basis $\{v_0, v_1, ..., v_n\}$. V has a cocommutative coalgebra structure determined by

$$\Delta(v_j) = \sum_{i=0}^{j} v_i \otimes v_{j-i}, \qquad j = 0, 1, ..., n,$$

$$\epsilon(v_j) = \delta_{j,0}, \qquad j = 0, 1, ..., n.$$

Consider $\mathrm{Hom}_{k^{1/p}}(V \otimes_k k^{1/p}, k^{1/p})$. As an algebra this is naturally isomorphic to $k^{1/p}[X]/\langle X^{n+1}\rangle$. If x^i denotes the coset of X^i then x^i corresponds to the $k^{1/p}$-linear map

$$V \otimes_k k^{1/p} \to k^{1/p}$$

$$v_r \otimes \lambda \to \lambda\delta_{r,i} \qquad r = 0, ..., n.$$

Thus if $n = pr$ and $\sum_{i=0}^{n} \lambda_i x^i \in k[X]/\langle X^{n+1}\rangle$ then

$$\left(\sum_{i=0}^{n} \lambda_i x^i\right)^p (v_n) = \lambda_r{}^p = \mathscr{F}(\lambda_r) = \mathscr{F}\left(\left(\sum_{i=0}^{n} \lambda_i x^i\right)(v_r \otimes 1)\right).$$

If $p \nmid n$ then

$$\left(\sum_{i=0}^{n} \lambda_i x^i\right)^p (v_n) = 0 = \mathscr{F}(0).$$

Thus

$$\mathscr{V}_V(v_n) = \begin{cases} 0 & \text{if } p \nmid n \\ v_{n/p} \otimes 1 & \text{if } p \mid n. \end{cases}$$

Since $V \to C$, $v_i \to c_i$, $i = 0,..., n$ is a coalgebra map, we are done by 4.1.5(a). Q.E.D.

4.2. *Birkhoff–Witt bialgebras*

In this section we utilize the coalgebra $B(U)$ on a vector space U. For details see [4, pages 261-271]. $B(U)$ is a graded cocommutative Hopf algebra where $B(U)(0) = k$ and $B(U)(1) = U$. We let $\pi : B(U) \to U$ be the natural projection onto the first graded component. $B(U)$ is characterized by the following universal property: if C is any cocommutative connected coalgebra, $C^+ = \operatorname{Ker} \epsilon_C$ and $f : C^+ \to U$ is a linear map then there is a unique coalgebra map $F : C \to B(U)$ with $\pi F = f$.

Let $N = \{0, 1, 2,...\}$ and let X be a basis for U. Let $N^{(X)} = \{f : X \to N \mid f$ has finite support, i.e., $f(x) = 0$ for almost all $x \in X\}$.

For $f \in N^{(X)}$ let $|f| = \sum_{x \in X} f(x)$. For $f, g \in N^{(X)}$ let $f + g \in N^{(X)}$ be defined by $(f + g)(x) = f(x) + g(x)$ for $x \in X$. Let $\binom{f}{g} = \prod_{x \in X} \binom{f(x)}{g(x)}$ where $\binom{a}{b} = 0$ if $b > a$. Since almost all of the terms in the product are $\binom{0}{0}$ which equals 1, $\binom{f}{g}$ makes sense.

It is shown in [4, p. 270] that $B(U)$ has a basis consisting of elements $\{u_{(f)} \mid f \in N^{(X)}\}$ where

$$\Delta[u_{(f)}] = \sum_{g+h=f} u_{(g)} \otimes u_{(h)} ,$$

$$\epsilon(u_{(f)}) = \delta_{f,0} , \qquad \text{(0 denotes the constant function zero)}$$

$$u_{(f)} u_{(g)} = \binom{f+g}{f} u_{(f+g)} ,$$

the unit is $u_{(0)}$.

Moreover the nth graded component $B(U)(n)$ has a basis consisting of $\{u_{(f)} \mid f \in N^{(X)}$ and $|f| = n\}$.

For $n \in N$ and $f \in N^{(X)}$ let $nf \in N^{(X)}$ be defined by $(nf)(x) = n(f(x))$ for all $x \in X$.

For $f \in N^{(X)}$ and $n \in N$ we write $n \mid f$ if there is $g \in N^{(X)}$ with $f = ng$. Then $n \mid f$ if and only if $n \mid f(x)$ for each $x \in X$. If it is not true that $n \mid f$ we write $n \nmid f$.

For $f \in N^{(X)}$ we let

$$\operatorname{Supp} f = \{x \in X \mid f(x) \neq 0\}$$

and for $x \in X$ we let $\delta_x \in N^{(X)}$ be defined by

$$\delta_x(y) = \begin{cases} 0 & \text{if } y \neq x \\ 1 & \text{if } y = x \end{cases}$$

for all $y \in X$. Then $u_{(\delta_x)}$ corresponds to $x \in X \subset U = B(U)(1)$.

4.2.1. PROPOSITION. (a) *For* $f, g \in N^{(X)}$ *with* $\operatorname{Supp} f \cap \operatorname{Supp} g = \varnothing$ *we have* $u_{(f)} u_{(g)} = u_{(f+g)}$.

(b) *For* $f \in N^{(X)}$, f *can be written "uniquely" in the form*

$$f = n_1 \delta_{x_1} + \cdots + n_r \delta_{x_r}$$

for some $\{x_i\} \subset X$ *and for each* i, $n_i \in N$.

$$u_{(f)} = u_{(n_1 \delta_{x_1})} \cdots u_{(n_r \delta_{x_r})}$$

(c) *If the characteristic of* k *is* $p > 0$ *and* $\mathscr{V} = \mathscr{V}_{B(U)}$ *then*

$$\mathscr{V}(u_{(f)}) = \begin{cases} 0 & \text{if } p \nmid f \\ u_{(g)} \otimes 1 & \text{if } p \mid f \text{ and } f = pg. \end{cases}$$

Proof. (a) follows from the multiplication formula. The first part of (b) is obvious and the second part of (b) follows from (a). (c) Observe that for any $x \in X$, $\{u_{(0\delta_x)}, u_{(1\delta_x)}, u_{(2\delta_x)}, \ldots\}$ is an ∞-sequence of divided powers in $B(U)$. Thus

$$\mathscr{V}(u_{(n\delta_x)}) = \begin{cases} 0 & \text{if } p \mid n \\ u_{(\frac{n}{p}\delta_x)} \otimes 1 & \text{if } p \mid n, \end{cases}$$

by (4.1.9). By (4.1.6, d) and the second part of (b) above we are done.

$B(U)$ is a graded coalgebra in the sense of [4, p. 228]. If $B(U)$ is given the filtration determined by

$$B(U)_n = \bigoplus_{i=0}^{n} B(U)(i)$$

then this filtration coincides with the filtration defined at the beginning of Section 3.2, [4, (11.2.1)]. If C is a cocommutative connected coalgebra then the filtration on C defined in the beginning of Section 3.2 is called the *coradical filtration.*

Suppose C is a subcoalgebra of $B(U)$. It follows from (3.2.1, b) that the coradical filtration on C is induced by that on $B(U)$, i.e., $C_n = C \cap B(U)_n$.

DEFINITION. A coalgebra $C \subset B(U)$ is called a *pseudosubbialgebra* if there is a cocommutative connected bialgebra H and an injective coalgebra map $\psi : H \to B(U)$ with $C = \operatorname{Im} \psi$.

4.2.2. PROPOSITION. *Suppose C is pseudosub-bialgebra of $B(U)$, $c \in C_n$ and $d \in C_m$.*

(a) *There is $e \in C_{n+m}$ where*

$$e - cd \in B(U)_{n+m-1}.$$

(b) *If the characteristic of k is $p > 0$ and $\mathscr{V}(c) = 0$ then e (as above) may be chosen with $\mathscr{V}(e) = 0$.*

Proof. Let H be a cocommutative connected bialgebra with $\psi : H \to B(U)$ an injective coalgebra map having $\operatorname{Im} \psi = C$. Then ψ is a coalgebra isomorphism between H and C and $\psi \mid H_i : H_i \to C_i$ is a coalgebra isomorphism for each i. Choose $x \in H_n$ and $y \in H_m$ with $\psi(x) = c$ and $\psi(y) = d$. Let $e = \psi(xy)$. By [4, pages 240-241]

$$\operatorname{gr} \psi : \operatorname{gr} H \to \operatorname{gr} B(U)$$

is a bialgebra map and thus

$$\psi(xy) - \psi(x)\,\psi(y) \in B(U)_{n+m-1}.$$

This proves (a).

If the characteristic of k is $p > 0$ then by (4.1.5, a)

$$0 = \mathscr{V}(c) = \mathscr{V}\psi(x) = (\psi \otimes I)\,\mathscr{V}_H(x).$$

Since ψ is injective it follows that $\psi \otimes I$ is injective and thus $\mathscr{V}_H(x) = 0$. By (4.1.5,a) and (4.1.6,d)

$$\mathscr{V}(e) = (\psi \otimes I)\,\mathscr{V}_H(xy) = (\psi \otimes I)(\mathscr{V}_H(x)\,\mathscr{V}_H(y)) = 0.$$

This proves (b).

We recall that for a cocommutative connected coalgebra C, $P(C)$ is defined to be $\{c \in C \mid \Delta(c) = c \otimes g + g \otimes c\}$ where g is the unique grouplike element of C. We have $P(C) \subset C_1$ and in fact

$$C_1 = P(C) \oplus kg.$$

For $B(U)$, $P(B(U)) = B(U)(1) = U$, [4, p. 261]. If C is a subcoalgebra of $B(U)$ then $P(C) \subset P(B(U)) = U$.

4.2.3. LEMMA. *As above suppose X is a basis for U. Let C be a pseudo-subbialgebra of $B(U)$ where $P(C) = U$. Let $c \in C_n$ and write*

$$c = \sum_i \lambda_i u_{(f_i)} + d$$

where $|f_i| = n$ for each i and $d \in B(U)_{n-1}$. Given any $x \in X$ there is an element

$$\tilde{c} = \sum_i \lambda_i f_i(x)\, u_{(f_i)} + e \in C_n$$

where $e \in B(U)_{n-1}$. Moreover if the characteristic of k is $p > 0$ we may also assume that $\tilde{c}$ satisfies $\mathscr{V}(\tilde{c}) = 0$.

Proof. Let $a^* \in B(U)^*$ be defined by $\langle a^*, u_{(f)}\rangle = 0$ if $f \neq \delta_x$ and $\langle a^*, u_{\delta_x}\rangle = 1$. Thus $\langle a^*, 1\rangle = 0$ and $a^* \in \mathscr{M} = 1^\perp$. Recall

$$L(a^*)c = \sum_{(c)} c_{(1)}\langle a^*, c_{(2)}\rangle \in C.$$

By (3.2.2,c) $L(a^*)d \in B(U)_{n-2}$. By the explicit form of the diagonalization of $u_{(f_i)}$ we have

$$L(a^*)\, u_{(f_i)} = \begin{cases} u_{(f_i - \delta_x)} & \text{if } x \in \operatorname{Supp}(f_i) \\ 0 & \text{if } x \notin \operatorname{Supp}(f_i). \end{cases}$$

Thus $L(a^*)c = \sum_i \lambda_i' u_{(f_i - \delta_x)} + \tilde{d} \in C_{n-1}$, where $\lambda_i' = \lambda_i$ if $f_i(x) > 0$, $\lambda_i' = 0$ if $f_i(x) = 0$ and $\tilde{d} \in B(U)_{n-2}$. Since $P(C) = U$ we have that $x \in C$. By (4.2.2,a) there is $\tilde{c} \in C_{(n-1)+1}$ with

$$(L(a^*)c)x - \tilde{c} \in B(U)_{n-1}.$$

By the explicit form of the multiplication in $B(U)$ we see that if $f_i(x) > 0$ then $u_{(f_i - \delta_x)} u_{\delta_x} = f_i(x)\, u_{(f_i)}$ and thus

$$(L(a^*)c)x = \sum_i \lambda_i f_i(x)\, u_{(f_i)} + \tilde{d}x$$

where $\tilde{d}x \in B(U)_{n-1}$. Thus $\tilde{c}$ is of the desired form. Moreover, by (4.2.2,b) if the characteristic of k is $p > 0$ we may assume that $\mathscr{V}(\tilde{c}) = 0$ since $\mathscr{V}(x) = 0$.
Q.E.D.

4.2.4. LEMMA. *Suppose the characteristic of k is $p > 0$ and C is a pseudo-subbialgebra of $B(U)$ with $P(C) = U$. Suppose $c \in C_n$ and*

$$c = \sum_i \lambda_i u_{(f_i)} + d$$

where $|f_i| = n$ *for each* i *and* $d \in B(U)_{n-1}$. *Then there is a* $c' \in C_n$ *with*

$$c' = \sum_{\substack{i \text{ where} \\ p/f_i}} \lambda_i u_{(f_i)} + d'$$

where $d' \in B(U)_{n-1}$ *and* $\mathscr{V}(c') = \mathscr{V}(c)$. *In particular if* $p \nmid f_i$ *for any* i *then* $c' \in B(U)_{n-1}$.

Proof. We give a procedure for eliminating the $\lambda_i u_{(f_i)}$ where $p \nmid f_i$. Suppose $p \nmid f_1$ then for some $x \in X$, $f_1(x) \not\equiv 0 \pmod p$. Thus by (4.2.3) there is an element

$$\tilde{c} = \sum_i \lambda_i f_i(x)\, u_{(f_i)} + e \in C_n$$

with $e \in B(U)_{n-1}$ and $\mathscr{V}(\tilde{c}) = 0$. Consider $c - \tilde{c}/f_1(x) \in C_n$. This is equal to

$$\sum_{i \neq 1} \lambda_i(1 - f_i(x)/f_1(x))\, u_{(f_i)} + (d - e/f_1(x))$$

where $d - e/f_1(x) \in B(U)_{n-1}$. For i where $p \mid f_i$ we have that $f_i(x) \equiv 0 \bmod p$ and so the coefficient $\lambda_i(1 - f_i(x)/f_1(x))$ is simply equal to λ_i. Since $\mathscr{V}(\tilde{c}) = 0$ we have that $\mathscr{V}(c - \tilde{c}/f_1(x)) = \mathscr{V}(c)$. Thus by iteration we are done.

4.2.5. LEMMA. *Suppose the characteristic of* k *is* $p > 0$, C *is a pseudo-sub-bialgebra of* $B(U)$, $P(C) = U$ *and* $c \in (C_n \otimes_k k^{1/p}) \cap \mathscr{V}(C)$. *Write*

$$c = \sum_i u_{(f_i)} \otimes \lambda_i + d$$

where $\{\lambda_i\} \subset k^{1/p}$, $|f_i| = n$ *for each* i *and* $d \in B(U)_{n-1} \otimes k^{1/p}$. *There is an element*

$$\bar{c} = \sum_i \lambda_i^p u_{(pf_i)} + e \in C_{pn}$$

where $e \in B(U)_{pn-1}$ *and* $\mathscr{V}(\bar{c}) = c$.

Proof. Choose $\bar{c} \in C$ where $\mathscr{V}(\bar{c}) = c$ and $\bar{c} \in C_r$ with r minimal. Write

$$\bar{c} = \sum_j \gamma_j u_{(g_j)} + z$$

where $|g_j| = r$ for each j and $z \in B(U)_{r-1}$. By (4.2.4) we may assume that for each j, $g_j = ph_j$. By the minimality of r we may assume that $\gamma_j \neq 0$ for each j. Note that $|g_j| = r$ and $g_j = ph_j$ implies that $r = ps$ where $s = |h_j|$ for each j. By (4.2.1,c)

$$\mathscr{V}(\bar{c}) = \sum_j u_{(h_j)} \otimes \gamma_j^{1/p} + \mathscr{V}(z).$$

We claim that $\mathscr{V}(z) \in B(U)_{s-1} \otimes_k k^{1/p}$. From (4.2.1,c) it follows that $\mathscr{V}(B(U)(t)) = 0$ if $p \nmid t$ and $\mathscr{V}(B(U))(t) \subset B(U)(t/p) \otimes_k k^{1/p}$ if $p \mid t$. Thus $\mathscr{V}(B(U)_t) \subset B(U)_{[t/p]} \otimes_k k^{1/p}$ where $[t/p]$ denotes the greatest integer not exceeding t/p. Thus if $r = ps$, $[r - 1/p] = s - 1$ and we have that $\mathscr{V}(z) \in B(U)_{s-1} \otimes_k k^{1/p}$.

By the equality of c and $\mathscr{V}(\bar{c})$ we have that $n = s$ and (possibly after reordering) $h_j = f_j$ and $\gamma_j^{1/p} = \lambda_j$ for each j. This completes the lemma.

4.2.6. THEOREM. *Suppose C is a pseudosub-bialgebra of $B(U)$ with $P(C) = U$.*

(a) *If the characteristic of k is zero then $C = B(U)$.*

(b) *If the characteristic of k is $p > 0$ then $C = B(U)$ if and only if $\mathscr{V} : C \to C \otimes_k k^{1/p}$ is surjective.*

Proof. We first show that if the characteristic is zero or greater than zero and $\mathscr{V}$ is surjective then $C = B(U)$. We proceed by induction showing that $C_n = B(U)_n$. Since $C \neq 0$ we have that $C_0 \neq 0$ so that $C_0 = k = B(U)_0$. Since $P(C) = U$ we have that

$$B(U)_1 = k \oplus U \subset C_0 \oplus P(C) = C_1 \subset B(U)_1$$

and $C_1 = B(U)_1$. Suppose by induction that $C_{n-1} = B(U)_{n-1}$ for some $n \geqslant 2$.

It suffices to show that for $f \in N^{(X)}$ where $|f| = n$ then $u_{(f)} \in C$. This is true by the form of the basis of $B(U)$. Suppose $f \in N^{(X)}$ and $\operatorname{Supp}(f)$ has more than one element. Then

$$f = n_1 \delta_{x_1} + \cdots + n_r \delta_{x_r}$$

for some $r > 1$ where $\sum n_i = n$ and $0 \leqslant n_i < n$ for each i. By the induction $u_{(n_i \delta_{x_i})} \in C$ for each i. By (4.2.2,a) there is $e \in C_n$ with

$$e - u_{(n_1 \delta_{x_1})} u_{(n_2 \delta_{x_2})} \cdots u_{(n_r \delta_{x_r})} \in B(U)_{n-1}.$$

Since $u_{(f)} = \prod_i u_{(n_i \delta_{x_i})}$ and $B(U)_{n-1} = C_{n-1}$ we have that $u_{(f)} \in C$.

Thus we may assume $u_{(f)} \in C$ whenever $|f| < n$ or $|f| = n$ and $\operatorname{Supp}(f)$ has more than one element. It remains to show that for each $x \in X$, $u_{(n\delta_x)} \in C$.

Case I. The characteristic is zero or $p > 0$ and $p \nmid n$. In this case $u_{(\delta_x)}$ and $u_{[(n-1)\delta_x]}$ lie in C and by (4.2.2,a) there is $e \in C_n$ with $e - u_{(\delta_x)} u_{((n-1)\delta_x)} \in B(U)_{n-1}$. Since $u_{(\delta_x)} u_{((n-1)\delta_x)} = n u_{(n\delta_x)}$, n is not a zero coefficient and $B(U)_{n-1} = C_{n-1}$ it follows that $u_{(n\delta_x)} \in C_n$ and we are done.

Case II. The characteristic is $p > 0$ and $n = pm$. In this case since $n \geqslant 2$ we have that $m \geqslant 1$. By the induction for any $x \in X$, $u_{(m\delta_x)} \in C_m$. By (4.2.5) and the assumption that $\mathscr{V}$ is surjective there is an element $\bar{c} \in C_n$ where $\mathscr{V}(\bar{c}) = u_{(m\delta_x)} \otimes 1$ and

$$\bar{c} = u_{(pm\delta_x)} + e$$

with $e \in B(U)_{n-1}$. Since $B(U)_{n-1} = C_{n-1}$ and $pm = n$ we have that $u_{(n\delta_x)} \in C$ and we are done.

Conversely we must show that if the characteristic is $p > 0$ and $C = B(U)$ then $\mathscr{V}$ is surjective. This is obvious because if

$$x = \sum_i u_{(f_i)} \otimes \lambda_i \in B(U) \otimes_k k^{1/p} \qquad \text{and} \qquad y = \sum_i \lambda_i{}^p u_{(pf_i)} \in B(U),$$

then $\mathscr{V}(y) = x$. Q.E.D.

4.2.7. Corollary. *Suppose H is a cocommutative connected bialgebra. Let $U = P(H)$.*

(a) *If the characteristic of k is zero then $H \cong B(U)$ as a coalgebra.*

(b) *If the characteristic of k is $p > 0$ then $H \cong B(U)$ as a coalgebra if and only if $\mathscr{V}_H : H \to H \otimes_k k^{1/p}$ is surjective.*

Proof. By [4, (12.1.1)] there is an injective coalgebra map $\psi : H \to B(U)$ where $\psi \mid P(H) : P(H) \to U$ is a linear isomorphism. Thus $C = \operatorname{Im} \psi$ is a pseudosub-bialgebra of $B(U)$ and $P(C) = \psi(P(H)) = U$.

If the characteristic of k is zero then $C = B(U)$ by the theorem and we have proved (a).

By (4.1.5,a) the $\mathscr{V}$ map of C is surjective if the $\mathscr{V}$ map of H is surjective. Thus by the theorem $C = B(U)$ if the $\mathscr{V}$ map of H is surjective. If $H \cong B(U)$ as a coalgebra then the $\mathscr{V}$ map of H is surjective since the $\mathscr{V}$ map of $B(U)$ is surjective. Q.E.D.

4.2.8. Corollary. *Suppose the characteristic of k is $p > 0$ and H is a cocommutative connected bialgebra over k. The following are equivalent:*

(i) *$H \cong B(U)$ as a coalgebra.*

(ii) *$H \otimes_k k^{1/p} \cong B(U) \otimes_k k^{1/p} = B_{k^{1/p}}(U \otimes_k k^{1/p})$ as a coalgebra.*

(iii) *$\mathrm{Hom}_{k^{1/p}}(H \otimes_k k^{1/p}, k^{1/p})$ is a domain.*

(iv) *$\mathrm{Hom}_{k^{1/p}}(H \otimes_k k^{1/p}, k^{1/p})$ is reduced, i.e., zero is the only nilpotent element.*

Proof. By $B_{k^{1/p}}(U \otimes_k k^{1/p})$ we mean the "B" bialgebra over $k^{1/p}$ of the

$k^{1/p}$ vector space $U \otimes_k k^{1/p}$. The natural equality of $B(U) \otimes_k k^{1/p}$ and $B_{k^{1/p}}(U \otimes_k k^{1/p})$ follows from the description of $B(U)$ in terms of a basis of U.

Clearly (i) implies (ii) and (iii) implies (iv). By [4, p. 278] (ii) implies (iii). Thus it remains to show that (iv) implies (i).

Suppose the map $\mathscr{V} : H \to H \otimes_k k^{1/p}$ is not surjective. Since $\mathscr{V}$ is $1/p$-linear its image is a $k^{1/p}$ subspace of $H \otimes_k k^{1/p}$. Thus we can choose $0 \neq f \in \mathrm{Hom}_{k^{1/p}}(H \otimes_k k^{1/p}, k^{1/p})$ where $\mathrm{Im}\, \mathscr{V} \subset \mathrm{Ker} f$. Then for any $h \in H$

$$f^p(h) = \mathscr{F}(f(\mathscr{V}(h))) = 0.$$

Since H spans $H \otimes_k k^{1/p}$ we have that $f^p = 0$ and $\mathrm{Hom}_{k^{1/p}}(H \otimes_k k^{1/p}, k^{1/p})$ is not reduced. This implies that $\mathscr{V}$ is surjective and by (4.2.7) we have that $H \cong B(U)$ as a coalgebra. Q.E.D.

Divided Powers

4.2.9. LEMMA. *Let C and D be coalgebras with $\{b_i\}$, $\{c_i\} \subset C$ and $\{d_i\} \subset D$ n-sequences of divided powers, where $0 \leqslant n \in \mathbb{Z}$ or $n = \infty$.*

(a) *In the tensor product coalgebra $C \otimes D$ if for $0 \leqslant t \leqslant n$*

$$e_t = \sum_{i=0}^{t} c_i \otimes d_{t-i}$$

then $\{e_t\}$ is an n-sequence of divided powers.

(b) *If $F : C \to D$ is a coalgebra map then $\{F(b_i)\} \subset D$ is an n-sequence of divided powers.*

(c) *If $\lambda \in k$ and for $0 \leqslant t \leqslant n$*

$$f_t = \{\lambda^t b_t\}$$

then $\{f_i\} \subset C$ is an n-sequence of divided powers.

(d) *If C is a bialgebra and for $0 \leqslant t \leqslant n$*

$$a_t = \sum_{i=0}^{t} b_i c_{t-i}$$

then $\{a_i\} \subset C$ is an n-sequence of divided powers.

Proof. (a), (b) and (c) are easily verified by calculation. (d) In the coalgebra $C \otimes C$ if for $0 \leqslant t \leqslant n$, $e_t = \sum_{i=0}^{t} b_i \otimes c_{t-i}$ then $\{e_t\} \subset C \otimes C$ is an n-sequence of divided powers by (a). The product map $p : C \otimes C \to C$ is a coalgebra map and $p(e_t) = a_t$ so that $\{a_t\}$ is an n-sequence of divided powers by (b). Q.E.D.

If H is a cocommutative connected bialgebra and $\{h_i\} \subset H$ is an n-sequence of divided powers then h_0 is a group-like element so that $h_0 = 1$. Thus $h_1 \in P(H)$. The n-sequence of divided powers $\{h_i\}$ is said to lie over h_1. By parts (d) and (c) of (4.2.9) we see that an n-sequence of divided powers lies over each element of $P(H)$ if and only if an n-sequence of divided powers lies over each element in a basis for $P(H)$. A cocommutative connected bialgebra H is popularly called a *Birkhoff-Witt* bialgebra if an ∞-sequence of divided powers lies over each element of $P(H)$.

$B(U)$ is a Birkhoff–Witt bialgebra since $\{u_{(i\delta_x)}\}$ is an ∞-sequence of divided powers which lies over x for each x in a basis for U. If the characteristic is zero then any cocommutative connected bialgebra H is Birkhoff–Witt since given $h \in P(H)$ the collection $\{h^i/i!\}$ is an ∞-sequence of divided powers lying over h.

Suppose H is a Birkhoff–Witt bialgebra. Let $U = P(H)$ and let X be a basis for U. For each $x \in X$ let $\{h_i^x\}$ be an ∞-sequence of divided powers lying over x, so that $h_0^x = 1$ and $h_1^x = x$. Totally order X and for each $f \in N^{(X)}$ let $h^{(f)}$ be the *ordered product*

$$\prod_{x \in X} h^x_{f(x)} \cdot$$

Since f has finite support almost all productands are 1 and $h^{(f)}$ makes sense. By [5, Theorem 3, p. 521] $\{h^{(f)} \in H \mid f \in N^{(X)}\}$ is a basis for H. Thus the linear map $B(U) \to H$, $u_{(f)} \to h^{(f)}$ for $f \in N^{(X)}$ is a linear isomorphism. It is a simple verification that this is a coalgebra map so that we have:

4.2.10. PROPOSITION. *A cocommutative connected Hopf algebra H is Birkhoff–Witt if and only if $H \simeq B(U)$ as a coalgebra.*

4.3 *Affine Hopf Algebras*

4.3.1. PROPOSITION. *Suppose that A is a commutative algebra over k of characteristic $p > 0$. The following statements are equivalent:*

1. *$A \otimes_k L$ is reduced for every reduced k algebra L.*
2. *$A \otimes_k k^{1/p}$ is reduced.*
3. *If $\{a_\alpha\} \subset A$ is any linearly independent set then $\{a_\alpha{}^p\}$ is a linearly independent set.*
4. *There is a basis $\{a_\alpha\}$ for A where $\{a_\alpha{}^p\}$ is a linearly independent set.*

Proof. Clearly (1) implies (2) and (3) implies (4).

Suppose $\{a_\alpha\} \subset A$ is a linearly independent set where $\{a_\alpha{}^p\}$ is not linearly independent. Write a non-trivial dependence relation $0 = \lambda_1 a_{\alpha_1}^p + \cdots + \lambda_n a_{\alpha_n}^p$ with $\{\lambda_i\} \subset k$. By the independence of $\{a_\alpha\}$ the element $\sum a_{\alpha_i} \otimes \lambda_i^{1/p}$ is a non-zero nilpotent element of $A \otimes_k k^{1/p}$. Thus (2) implies (3).

Let $\{a_\alpha\}$ be a basis for A as in (4). For $\sum a_{\alpha_i} \otimes \lambda_i = x \in A \otimes_k L$ the pth power is $\sum a_{\alpha_i}^p \otimes \lambda_i{}^p$. Since $\{a_\alpha{}^p\}$ is linearly independent x^p cannot be zero unless each $\lambda_i{}^p$ is zero. Since L is reduced this implies that each $\lambda_i = 0$ and $x = 0$. Clearly $A \otimes_k L$ having no non-zero pth power nilpotent elements implies that $A \otimes_k L$ is reduced. Thus (4) implies (1). Q.E.D.

DEFINITION. If A is a commutative k algebra then A is called absolutely reduced if $A \otimes_k \bar{k}$ is reduced.

Certainly A is reduced if it is absolutely reduced, and by (4.3.1) if the characteristic of k is $p > 0$ then A is absolutely reduced if $A \otimes_k k^{1/p}$ is reduced.

4.3.2. PROPOSITION. *Suppose that A is a finitely generated commutative algebra where the characteristic of k is $p > 0$ and A is absolutely reduced. Let A^0 be the coalgebra dual to A as described in Section* 1.3. (*A^0 is cocommutative because A is commutative.*) *Then $\mathscr{V} : A^0 \to A^0 \otimes_k k^{1/p}$ is surjective.*

Proof. Since $A \otimes_k k^{1/p}$ is reduced the $\mathscr{F}$ map is injective. The image of the $\mathscr{F}$ map is $kA^{(p)} \otimes_k k \subset A \otimes_k k^{1/p}$, where $kA^{(p)}$ is the k-subalgebra of A generated by $A^{(p)}$. Thus

$$F : A \otimes_k k^{1/p} \to kA^{(p)}$$
$$a \otimes \lambda \to \lambda^p a^p$$

is a bijective p-linear map.

There is a natural inclusion of $A^0 \subset A^*$ and so there is a natural inclusion

$$A^0 \otimes_k k^{1/p} \subset \operatorname{Hom}_{k^{1/p}}(A \otimes_k k^{1/p}, k^{1/p}).$$

Under this inclusion

$$A^0 \otimes_k k^{1/p} \subset (A \otimes_k k^{1/p})^0$$

where the "0" on $(A \otimes_k k^{1/p})$ is with respect to the field $k^{1/p}$. This is true because if $\{f_i\} \subset A^0$ and for each i, J_i is a cofinite ideal of A with $J_i \subset \operatorname{Ker} f_i$, then $J = \bigcap J_i$ is a cofinite ideal in A with $J \subset \operatorname{Ker} f_i$ for each i. The ideal $J \otimes_k k^{1/p}$ of $A \otimes_k k^{1/p}$ is cofinite and lies in the kernel of $\sum f_i \otimes \lambda_i$ where $\{\lambda_i\} \subset k^{1/p}$.

Suppose $d \in A^0 \otimes_k k^{1/p}$. We define a map $e : kA^{(p)} \to k$ as the composite

$$kA^{(p)} \xrightarrow{F^{-1}} A \otimes_k k^{1/p} \xrightarrow{d} k^{1/p} \xrightarrow{\mathscr{F}} k.$$

Since F is p-linear, F^{-1} is $1/p$-linear. d is linear and $\mathscr{F}$ is p-linear. Thus e is linear. Since $d \in A^0 \otimes_k k^{1/p}$ there is a cofinite (with respect to the field $k^{1/p}$) ideal $J \subset A \otimes_k k^{1/p}$ with $J \subset \operatorname{Ker} d$. Since F is a p-linear algebra isomorphism from $A \otimes_k k^{1/p}$ to $kA^{(p)}$ it follows that $F(J)$ is a cofinite (with respect to the field k) ideal of $kA^{(p)}$. Clearly $F(J) \subset \operatorname{Ker} e$. Thus $e \in (kA^{(p)})^0$, the "0" with respect to k.

The inclusion $kA^{(p)} \xhookrightarrow{i} A$ induces $A^0 \xrightarrow{i^0} (kA^{(p)})^0$. Since A is a finitely generated algebra so is $kA^{(p)}$. Thus $kA^{(p)}$ is noetherian. A is integral over $kA^{(p)}$ since any element $a \in A$ satisfies $X^p - a^p$. Since A is a finitely generated algebra it is a finitely generated $kA^{(p)}$-module [6, p. 254]. Then by (1.3.10) the coalgebra map i^0 is surjective. Choose $f \in A^0$ where $i^0(f) = e$. We will now show that $\mathscr{V}(f) = d$. The map $\psi : A \otimes_k k^{1/p} \to \operatorname{Hom}_{k^{1/p}}(A^0 \otimes_k k^{1/p}, k^{1/p})$ is defined by

$$\psi(a \otimes \gamma)(a^0 \otimes \lambda) = \lambda\gamma\langle a^0, a\rangle$$

where $a \otimes \gamma \in A \otimes_k k^{1/p}$ and $a^0 \otimes \lambda \in A^0 \otimes_k k^{1/p}$. The map ψ is an algebra map. Considering A as $A \otimes_k k \subset A \otimes_k k^{1/p}$ it is not difficult to show that $\psi(A)$ is a dense subset of $\operatorname{Hom}_{k^{1/p}}(A^0 \otimes_k k^{1/p}, k^{1/p})$ in the sense of (4.1.7,b). For any $a \in A$

$$\psi(a)^p(f) = f(a^p) = e(a^p) = \mathscr{F}\, d(a) = \mathscr{F}(\psi(a)(d)).$$

Thus by (4.1.7,b), $\mathscr{V}(f) = d$. Q.E.D.

Recall $\mathscr{D}_\epsilon^{\,n}(A) = (\mathscr{M}^{n+1})^\perp \subset A^*$ where A is a commutative algebra and $\epsilon : A \to k$ is an algebra map with kernel $\mathscr{M}$, (2.3.1). $\mathscr{D}_\epsilon(A)$ denotes $\bigcup \mathscr{D}_\epsilon^{\,n}(A) \subset A^*$. By (2.4.2) $\mathscr{D}_\epsilon(A)$ is a sub-bialgebra of A^0 if A is a commutative bialgebra with augmentation ϵ and $\operatorname{Ker} \epsilon = \mathscr{M}$ is a finitely generated ideal. By (3.5.9,a), $\mathscr{D}_\epsilon(A)$ is the connected component of k in A^0.

$\mathscr{D}_\epsilon^{\,n}(A)$ is a finite dimensional subcoalgebra of A^0; the dual algebra to $\mathscr{D}_\epsilon^{\,n}(A)$ is $A/\mathscr{M}^{n+1}$. Thus as algebras

$$\begin{aligned}\mathscr{D}_\epsilon(A)^* &= \operatorname{Hom}_k\Big(\bigcup_n \mathscr{D}_\epsilon^{\,n}(A), k\Big)\\ &= \varprojlim \operatorname{Hom}_k(\mathscr{D}_\epsilon^{\,n}(A), k)\\ &= \varprojlim A/\mathscr{M}^{n+1} = \hat{A},\end{aligned}$$

where by $\hat{A}$ we mean the completion of A in the $\mathscr{M}$-adic topology.

4.3.3. PROPOSITION. *Suppose that A is a commutative bialgebra where $\mathscr{M} = \operatorname{Ker} \epsilon$ is a finitely generated ideal. Then $\hat{A} \simeq k[[X_1, ..., X_n]]$ as algebras if and only if $\mathscr{D}_\epsilon(A) \simeq B(U)$ as coalgebras where U is an n-dimensional space.*

Proof. If $\mathscr{D}_\epsilon(A) \simeq B(U)$ as a coalgebra then $\hat{A} = \mathscr{D}_\epsilon(A)^* \simeq B(U)^*$ as an algebra and $B(U)^*$ is a power series ring in the same number of variables as the dimension of U, [4, p. 278].

Conversely if $\mathscr{D}_\epsilon(A)^* = \hat{A} \cong k[[X_1, ..., X_n]]$ as an algebra then $\mathscr{D}_\epsilon(A)^*$ is noetherian and so by [2], the natural coalgebra map $\mathscr{D}_\epsilon(A) \to \mathscr{D}_\epsilon(A)^{*0}$ is surjective. Therefore one has $\mathscr{D}_\epsilon(A) = \hat{A}^0$ which is isomorphic to $k[[X_1, ..., X_n]]^0$ as a coalgebra. If U is an n-dimensional vector space then $B(U)^* \cong k[[X_1, ..., X_n]]$ as an algebra [4, p. 278] so by the same reasoning as above $B(U) \cong k[[X_1, ..., X_n]]^0$ as a coalgebra. Thus $\mathscr{D}_\epsilon(A) \cong B(U)$ as a coalgebra. Q.E.D.

Suppose that A is a commutative bialgebra where $\mathscr{M} = \operatorname{Ker} \epsilon$ is a finitely generated ideal. Let L be a field extension of k. The L bialgebra $A \otimes_k L$ has augmentation $\epsilon \otimes I$ and finitely generated augmentation ideal $\mathscr{M} \otimes_k L$. Thus we have $\mathscr{D}_{\epsilon \otimes I}(A \otimes_k L)$ the connected component of L in $(A \otimes_k L)^0$, the "0" with respect to the field L.

4.3.4. Proposition. (a) *If A is a commutative bialgebra where $\mathscr{M} = \operatorname{Ker} \epsilon$ is a finitely generated ideal and L is a field extension of k then $\mathscr{D}_{\epsilon \otimes I}(A \otimes_k L) \cong \mathscr{D}_\epsilon(A) \otimes_k L$ as bialgebras.*

(b) *If A is a finitely generated commutative Hopf algebra where $\mathscr{D}_\epsilon(A) \cong B(U)$ as a coalgebra then $A \otimes_k L$ is a reduced L algebra for any field extension L of k.*

Proof. We have the map $\tau : \mathscr{D}_\epsilon(A) \otimes_k L \to \operatorname{Hom}_L(A \otimes_k L, L)$ where for $x \otimes \lambda \in \mathscr{D}_\epsilon(A) \otimes_k L$, $a \otimes \gamma \in A \otimes_k L$ $\langle \tau(x \otimes \lambda), a \otimes \gamma \rangle = \lambda\gamma\langle x, a \rangle$. Clearly τ is an injective algebra map. For $z \in \mathscr{D}_\epsilon(A) \otimes_k L$, z actually lies in $\mathscr{D}_\epsilon{}^n(A) \otimes_k L$ for some n. Then $\operatorname{Ker} \tau(z) \supset \mathscr{M}^{n+1} \otimes_k L = (\mathscr{M} \otimes_k L)^{n+1}$ and so $\tau(z) \in \mathscr{D}^n_{\epsilon \otimes I}(A \otimes_k L)$. Considering τ as a map $\tau : \mathscr{D}_\epsilon(A) \otimes_k L \to \mathscr{D}_{\epsilon \otimes I}(A \otimes_k L)$ it is clearly an injective bialgebra map. $\tau \mid (\mathscr{D}_\epsilon{}^n(A) \otimes_k L)$ has the factoring

$$
\begin{aligned}
\mathscr{D}_\epsilon{}^n(A) \otimes_k L &\xrightarrow{\cong} \operatorname{Hom}_k(A/\mathscr{M}^{n+1}, k) \otimes_k L \\
&\xrightarrow{\cong} \operatorname{Hom}_k(A/\mathscr{M}^{n+1}, L) \xrightarrow{\cong} \operatorname{Hom}_L((A/\mathscr{M}^{n+1}) \otimes_k L, L) \\
&\xrightarrow{\cong} \operatorname{Hom}_L((A \otimes_k L)/(\mathscr{M}^{n+1} \otimes_k L), L) \\
&\xrightarrow{\cong} \operatorname{Hom}_L((A \otimes_k L)/(\mathscr{M} \otimes_k L)^{n+1}, L) \xrightarrow{\cong} \mathscr{D}^n_{\epsilon \otimes I}(A \otimes_k L),
\end{aligned}
$$

so is an isomorphism. (The second map is an isomorphism because $A/\mathscr{M}^{n+1}$ is finite dimensional over k.) Thus τ is an isomorphism.

(b) If $\bar{L}$ is the algebraic closure of L then it suffices to prove that $A \otimes_k \bar{L}$ is reduced since $A \otimes_k \bar{L} \supset A \otimes_k L$. Thus we may assume that L is algebraically closed.

Clearly $A \otimes_k L$ is a finitely generated commutative Hopf algebra over L. Part (a) of the proposition gives the first isomorphism in the chain of *coalgebra* isomorphisms:

$$\mathscr{D}_{\epsilon\otimes I}(A \otimes_k L) \cong \mathscr{D}_\epsilon(A) \otimes_k L \cong B(U) \otimes_k L \cong B_L(U \otimes_k L).$$

Thus $A \otimes_k L$ satisfies the same hypotheses over L as A does over k. Thus it suffices to prove that A is reduced assuming that k is algebraically closed.

By (1.3.7) A is proper algebra and the natural algebra map $\rho : A \to A^{0*}$, $\langle \rho(a), a^0 \rangle = \langle a^0, a \rangle$ is injective. Thus it suffices to prove that A^{0*} is reduecd. By (3.5.9,c) and (3.1.1,b) we have that as coalgebras

$$A^0 \cong \coprod_{g \in G(A^0)} \mathscr{D}_\epsilon(A) \cong \coprod_{g \in G(A^0)} B(U).$$

Thus as algebras

$$A^{0*} \cong \prod_{g \in G(A^0)} B(U)^*$$

which is the product of domains by [4, p. 278] and certainly is reduced. This completes the proposition.

4.3.5. Lemma. *Suppose that A is a commutative algebra with augmentation $\epsilon : A \to k$ and $\mathscr{M} =$ Ker ϵ is a finitely generated ideal. Then the dimension of $P(\mathscr{D}_\epsilon(A))$ is finite.*

Proof. By (3.4.2), $\mathscr{D}_\epsilon(A)$ is connected so that $P(\mathscr{D}_\epsilon(A))$ makes sense. By [4, (10.0.1)], $\mathscr{D}_\epsilon(A)_1 = k\epsilon \oplus P(\mathscr{D}_\epsilon(A))$. By (3.4.2) the coradical filtration on $\mathscr{D}_\epsilon(A)$ corresponds to the $\mathscr{M}$-adic filtration, so that $\mathscr{D}_\epsilon(A)_1 = (\mathscr{M}^2)^\perp$. By (1.3.9), $\mathscr{M}^2$ is cofinite in A; hence $\mathscr{D}_\epsilon(A)_1$ and $P(\mathscr{D}_\epsilon(A))$ are finite dimensional.

Q.E.D.

4.3.6. Theorem. *Suppose that A is a finitely generated commutative bialgebra.*

(a) *If the characteristic of k is zero then*

(i) *$\hat{A}$ is a power series ring over k,*

(ii) *$\mathscr{D}_\epsilon(A)$ is a Birkhoff–Witt bialgebra,*

(iii) *$\mathscr{D}_\epsilon(A) \cong B(U)$ as coalgebras for finite dimensional U,*

(iv) *if A has an antipode then $A \otimes_k L$ is reduced for any field extension L of k.*

(b) *If the characteristic of k is $p > 0$ then the following are equivalent*:

(i) $\hat{A}$ *is a power-series ring over k*,

(ii) $\mathscr{D}_\epsilon(A)$ *is a Birkhoff–Witt bialgebra*,

(iii) $\mathscr{D}_\epsilon(A) \cong B(U)$ *as coalgebras for finite dimensional U*,

(iv) $\mathscr{V} : \mathscr{D}_\epsilon(A) \to \mathscr{D}_\epsilon(A) \otimes_k k^{1/p}$ *is surjective*,

(v) $\widehat{A \otimes_k k^{1/p}}$ is a power series ring over $k^{1/p}$,

(vi) $\widehat{A \otimes_k k^{1/p}}$ is reduced.

Conditions (i)-(vi) *are implied by A being absolutely reduced and if A has an antipode then conditions* (i)-(vi) *imply that A is absolutely reduced.*

Proof. By (4.3.5.) the U in part (iii) of both (a) and (b) must be finite dimensional. By (4.3.3.) (i) is equivalent to (iii) and by (4.2.10) (ii) is equivalent to (iii), in both parts (a) and (b).

By (4.2.7,a) (a,(iii)) holds. By (4.3.4.), (a,(iv)) holds. This proves (a).

(b) By (4.3.4.), $\mathscr{D}_{\epsilon\otimes I}(A \otimes_k k^{1/p}) \cong \mathscr{D}_\epsilon(A) \otimes_k k^{1/p}$ as bialgebras and so

$$\widehat{A \otimes_k k^{1/p}} = \mathrm{Hom}_{k^{1/p}}(\mathscr{D}_{\epsilon\otimes I}(A \otimes_k k^{1/p}), k^{1/p}) \cong \mathrm{Hom}_{k^{1/p}}(\mathscr{D}_\epsilon(A) \otimes_k k^{1/p}, k^{1/p})$$

as algebras. Thus (vi) implies (iii) by (4.2.8). Clearly (v) implies (vi). If (iii) holds then as algebras

$$\begin{aligned}\widehat{A \otimes_k k^{1/p}} &\cong \mathrm{Hom}_{k^{1/p}}(\mathscr{D}_\epsilon(A) \otimes_k k^{1/p}, k^{1/p})\\ &\cong \mathrm{Hom}_{k^{1/p}}(B(U) \otimes_k k^{1/p}, k^{1/p}) \cong \mathrm{Hom}_{k^{1/p}}(B_{k^{1/p}}(U \otimes_k k^{1/p}), k^{1/p})\end{aligned}$$

which is a power series ring by [4, p. 278]. Thus (iii) implies (v). By (4.2.7) (iii) is equivalent to (iv). Thus (i)-(vi) are equivalent.

Suppose that A is absolutely reduced. By (4.3.2), $\mathscr{V} : A^0 \to A^0 \otimes_k k^{1/p}$ is surjective. Since A^0 is cocommutative we can write it as the direct sum of its irreducible components

$$A^0 = \coprod A_i^0$$

by (3.1.2,c). Since $\mathscr{D}_\epsilon(A)$ is the connected component of k, we can collect the other components and write $A^0 = \mathscr{D}_\epsilon(A) \oplus C$. By (4.1.5,c), $\mathscr{V}_{A^0} = \mathscr{V}_{\mathscr{D}_\epsilon(A)} \oplus \mathscr{V}_C$. Since $\mathscr{V}_{A^0}$ is surjective we have that $\mathscr{V}_{\mathscr{D}_\epsilon(A)}$ is surjective. Then by (4.2.7,b), $\mathscr{D}_\epsilon(A) \cong B(U)$ as a coalgebra. We have already observed that U must be finite dimensional. Thus condition (iii) and the other equivalent conditions are satisfied.

If A has an antipode then by (4.3.4,b) condition (iii) implies that A is absolutely reduced. Q.E.D.

When the characteristic of k is $p > 0$ but k is perfect, $k = k^{1/p}$. By (4.3.1) A is reduced if and only if it is absolutely reduced. Also the "$\otimes_k k^{1/p}$" disappears in conditions (iv)-(vi) part (b).

References

1. C. Chevalley, "Fundamental Concepts of Algebra," Academic Press, New York, 1956.
2. R. Heyneman, "Coalgebras of Finite Type," to appear.
3. R. Heyneman and M. E. Sweedler, Affine Hopf Algebras I, *J. Algebra*, **13** (1969), 192–241.
4. M. E. Sweedler, Hopf Algebras, Benjamin, New York, 1969.
5. M. E. Sweedler, Hopf algebras with one grouplike element, *TAMS* **127** (1967), 515–526.
6. O. Zariski and P. Samuel, "Commutative Algebra," Volume I, Van Nostrand, Princeton, 1958.